17. Protocols and Servers

🌐 Network Protocols

1. What is the Purpose of the NFS Protocol?

- **NFS (Network File System)** allows clients to access files over a network **as if they were local**.
- Originally developed by Sun Microsystems.
- Commonly used in UNIX/Linux environments for **centralized storage and sharing**.
- Purpose:
  - Share directories and files between systems over a LAN.
  - Enable collaborative work on shared files without duplication.

2. How Does SMTP Work to Send Emails?

- **SMTP (Simple Mail Transfer Protocol)** is used to **send and relay email** between mail servers.
- **How it works:**
  1. **Client (MUA)** sends an email to the **SMTP server (MSA)**.
  2. The server **relays** the email through one or more **Mail Transfer Agents (MTA)**.
  3. Eventually reaches the **recipient's mail server (MDA)**.
  4. The recipient retrieves email using **IMAP or POP3**.
- Works on **port 25** (or 587 for authenticated, encrypted submission).

3. What Information Does SNMP Provide About Network Devices?

- **SNMP (Simple Network Management Protocol)** provides monitoring and management data for network devices.
- Can retrieve:
  - CPU and memory usage
  - Network interface status
  - Uptime
  - Bandwidth stats
  - Configuration details
- Devices expose data through **MIBs (Management Information Bases)**.
- Works over **UDP port 161**.

4. How Does SMB Enable File Sharing Between Different Operating Systems?

- **SMB (Server Message Block)** allows sharing of files, printers, and serial ports over a network.
- Used primarily in **Windows systems**, but **Linux can use it via Samba**.
- SMB operates over **port 445**.
- Enables cross-platform file sharing by:
  - Handling authentication
  - Managing file locks and sessions
  - Mapping remote shares to local drives

---

5. What Is the Role of LDAP in Authentication and Authorization?

- **LDAP (Lightweight Directory Access Protocol)** is used to access and manage directory information services over IP.
- Commonly used for:
  - **Centralized authentication**
  - Storing user credentials and permissions
- Role:
  - Verify user identities (authentication)
  - Check group membership or roles (authorization)
- Works on **port 389** (or **636** for LDAPS — secure version)

---

6. Explain the Security Risks Associated with Using RDP

- **RDP (Remote Desktop Protocol)** allows remote access to desktops, mainly in Windows.
- Risks:
  - **Brute-force attacks** on exposed RDP ports (default: 3389)
  - **Credential theft** via weak or reused passwords
  - **RDP vulnerabilities** like BlueKeep (CVE-2019-0708)
  - **Man-in-the-middle (MitM)** attacks if encryption isn't enforced
  - **Lateral movement** inside networks after compromise

---

7. Differentiate Between Secure Protocols Like HTTPS and SFTP from Their Insecure Counterparts

Protocol	Secure Version	Insecure Version	Difference
Web	HTTPS (443)	HTTP (80)	Encrypts traffic using TLS

Protocol	Secure Version	Insecure Version	Difference
File Transfer	SFTP (22)	FTP (21)	SFTP uses SSH; FTP is plaintext
Email Sending	SMTPS (465/587)	SMTP (25)	SMTPS uses TLS/SSL
Remote Access	SSH (22)	Telnet (23)	SSH encrypts; Telnet is plaintext

Secure protocols ensure:

- Encryption
- Integrity
- Authentication

8. Explain the Benefits of Using SSH for Secure Remote Access

- **SSH (Secure Shell)** provides **encrypted and authenticated** remote access over **port 22.**
- Benefits:
  - **Encryption** of entire session (prevents sniffing)
  - **Public key authentication**
  - **Tunneling** other protocols securely (e.g., RDP, VNC)
  - **File transfers** via `scp` or `sftp`
  - **Port forwarding** and reverse tunnels for secure services

9. Explain the Concept of Port Numbers and Their Significance in Network Communication

- **Ports** identify specific services or applications on a host.
- Format: `IP:Port` (e.g., 192.168.0.1:80)
- Types:
  - **Well-known ports** (0–1023): Reserved for standard services (HTTP, DNS, SSH)
  - **Registered ports** (1024–49151): For vendor-specific services
  - **Dynamic/private ports** (49152–65535): Used by clients temporarily

Significance:

- Allow multiple services to run on the same IP
- Help firewalls and scanners identify running services

10. Differentiate Between Different Types of Network Encryption Protocols

Protocol	Layer	Usage	Encryption Example
SSL/TLS	Application	HTTPS, IMAPS, SMTPS	AES, RSA, ECC
IPsec	Network	VPNs, Secure tunneling	AH, ESP with AES or 3DES
WPA2/WPA3	Data Link	Wi-Fi encryption	AES-CCMP
SSH	Application	Remote access, tunneling	AES for data, RSA/ECDSA for auth

11. Explain the Importance of Keeping Network Protocols Up-to-Date and Patched

- **Why it matters:**
  - Fix **known vulnerabilities** (e.g., Heartbleed in SSL)
  - Improve **security standards** (e.g., TLS 1.3 vs TLS 1.0)
  - Protect against **exploit kits** targeting outdated services
  - Ensure **compatibility** with modern secure clients
- **Unpatched protocols** are a **major attack vector** in real-world breaches.
- Tools like `nmap`, `sslscan`, and vulnerability scanners can detect outdated or vulnerable versions.